USPTO Privacy Impact Assessment Statement

USPTO Identification and Security Access Control Systems (Badging and Access System)

Prepared by: J.R. Garland, Security Office

Reviewed by: David J. Freeland, Chief Information Officer

1. **What information is to be collected (e.g., nature and source)?**

   Information collected may include the individual's name, organization, work telephone number, date of birth, agency identification (employee) number, and photographic image.

   Collected information may also include a copy of an applicant's Social Security Card, driver's license and passport. These documents are used to verify the individual's identity.

   Applicants include USPTO employees, contractors and select outside persons, such as search room users, and frequent visitors from other agencies.

   The source(s) of collected information are the Standard Forms 85, 85P and 86 (Questionnaires for Non-Sensitive Positions, Public Trust Positions and National Security Positions, respectively); Standard Form 171, Application for Federal Employment; Optional Forms 306 and 612 (Federal Declaration for Employment and Optional Application for Federal Employment, respectively); OFI Form 86C (Special Agreement Check); PIV Request Form, and the SF 87 and FD 258 Fingerprint cards.

2. **Why is the information being collected (e.g., to determine eligibility)?**

   The information is used to verify the individual's identity, and pursuant to Executive Orders 10450 and Executive Order 12968, to initiate background investigations of an appropriate level by the U.S. Office of Personnel Management (OPM).

3. **What is the intended use of the information (e.g., to verify existing data)?**

   To restrict entry to installations and activities, to ensure positive identification of personnel authorized to access restricted areas, and maintain accountability for issuance and disposition of security/access badges and similar physical access tools.

4. **With whom will the information be shared (e.g., another agency for a specified programmatic purpose)?**

   The information is not automatically shared with outside agencies, but may be used as set forth in the Privacy Act System of Records Notice (see item 7 below).

   Routine Uses include those in the Prefatory Statement of General Routine Uses Nos. 1-13, as found at 46 FR 63501-63502 (December 31, 1981).

5. What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how do individuals grant consent?

Each individual is presented the opportunity to decline or sign a release when completing the background investigative forms. These forms also note the authority for collecting the information, and that all collected information is protected under the Provisions of the Privacy Act.

Individuals are informed that giving personal information is voluntary. However, they are also informed that if their identity cannot be verified, or the background investigation required by Executive Orders 10450 or 12968 cannot be completed, or completed it in a timely manner, their placement or employment prospect may be affected.

6. How will the information be secured (e.g., administrative and technological controls)?

Management Controls:
System users include USPTO Security and Safety Division employees, and authorized members of the contract security guard force. The level of access to the system is determined based on the user's job function and office policy, and authorized by the USPTO Security Office.

Operational Controls:
Information and information storage systems are located within secure, restricted access areas, staffed by a contract security guard force or protected by intrusion detection devices during non-business hours.

All hardware associated with this system is physically locked down. The USPTO Security Service Center and the Security and Safety Division office are staffed continuously during business hours. Both areas are protected by intrusion detection devices during non-business hours and access is controlled by access card entry. The back-up system, which mirrors the primary in the Security Service Center, is located in a separate facility and is protected by intrusion detection devices 24 hours a day.

Technical Controls:
The database is a stand-alone system within the USPTO network, supported by a "mirrored" system, another a stand-alone system which continuously backs up the primary database. OCIO established technical controls include password authentication at the server and database levels.

7. Is a system of records being created under the Privacy Act, 5 U.S.C. 552a?

No, there is no new system of records being created. Existing systems of records cover the information residing in the databases. This includes:

COMMERCE/PAT-TM-18, USPTO Identification and Security Access Control Systems. The relevant System of Records Notice was published in the *Federal Register*, 69 FR 74502-74503 (December 14, 2004).

A system of records under 5 U.S.C. 552a is defined as "a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

Prepared and Approved by — Date
J. R. Garland

I have reviewed and approve the attached Privacy Impact Assessment document(s).

David J. Freeland — Date
Chief Information Officer

cc:
Griffin Macy, Deputy Chief Information Officer
David Larsen, Acting Director, Enterprise IT and Security Management

Attachments